Le Wi-Fi : série de fiches pratiques réalisées pour l'Observatoire des droits de l'internet

Robert, Romain

Publication date:
2008

Document Version
le PDF de l'éditeur

Le Wi-Fi - Entreprise@Web: Questions

"Qu'est-ce que le Wi-Fi?"

"Dois-je protéger mon accès Wi-Fi contre les intrusions non désirées?"

"Comment me protéger contre les accès non autorisés?"

"Comment installer un hotspot dans mon magasin au profit de mes clients?"

Fiche pratique

Qu'est-ce que le Wi-Fi ?

Le Wi-Fi (pour « Wireless Fidelity ») est une technique de communication en réseau local sans fil. Cette technique permet une connexion à haut débit entre des ordinateurs et des terminaux et est devenue un autre moyen d'accéder à Internet à haut débit.

Equipé d'une carte Wi-Fi (intégrée ou externe), votre ordinateur peut communiquer avec d'autres terminaux ou accéder à Internet avec une vitesse de connexion pouvant dépasser les 10 Mbps. Certains appareils portables, comme par exemple un téléphone portable ou un lecteur MP3 de dernière génération, sont également équipés d'une telle technologie.

La portée des ondes Wi-Fi étant relativement réduite (plusieurs dizaines de mètres), cette norme est destinée à l'établissement d'un réseau sans fil local (contrairement au réseau GSM ou 3G par exemple).

La technologie Wi-Fi peut être utilisée à des fins purement domestiques (par exemple pour l'établissement d'un réseau local pour accéder sans fil à Internet). Il présente ainsi l'avantage de ne plus devoir tirer une multitude de câbles dans toute la maison pour surfer à plusieurs, ou pour relier votre ordinateur au modem ou à d'autres ordinateurs.

Par ailleurs, de plus en plus de fournisseurs d'accès à Internet et d'établissements divers (cafés, magasins, aéroports, bibliothèques…) installent des points d'accès Wi-Fi (ou « bornes Wi-Fi ») afin de permettre un accès à Internet haut débit dans les lieux publics. Ces lieux sont appelés hotspots et sont répertoriés sur Internet ou renseignés sur les lieux d'accès.

Auteurs: FUNDP-CRID sous la coordination de Romain Robert

Fiche pratique

@ Entreprise WEB

Dois-je protéger mon accès Wi-Fi contre les intrusions non désirées ?

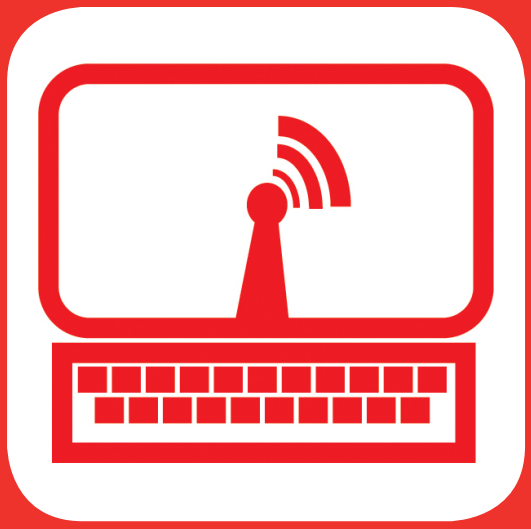
Outre le fait qu'une intrusion sur votre réseau peut consommer une partie de la capacité maximum mensuelle allouée par votre fournisseur d'accès, un accès non sécurisé attirera souvent les criminels informatiques, ce qui rendra difficile, voire impossible, l'identification de l'auteur de l'infraction.

En outre, sachez que la loi oblige toute personne qui traite des données à caractère personnel (fichiers clients, données médicales, etc.) à sécuriser le traitement en fonction des risques encourus et de la nature des données traitées. L'installation de moyens de prévention contre les intrusions dans votre système via le Wi-Fi peut donc être une étape encore plus importante pour certaines personnes ou organismes traitant des données sensibles (cabinets d'avocats, hôpitaux, etc.).

Auteurs: FUNDP-CRID sous la coordination de Romain Robert

Fiche pratique

Comment me protéger contre les accès non autorisés ?



Certains surfeurs sur Internet sont passés maîtres dans l'art de pénétrer les systèmes informatiques connectés au réseau, parfois par jeu, pour relever un défi ou, tout simplement, pour nuire ou semer la pagaille. Il serait naïf de vous croire à l'abri de pareils agissements, sous prétexte que vous n'avez rien à vous reprocher ou que votre système ne contient rien de bien extraordinaire.

De manière générale, pour vous protéger, le mieux est d'installer un firewall (pare-feu), c'est-à-dire un dispositif, logiciel ou matériel, destiné précisément à dresser un mur de sécurité entre votre système et le reste du réseau, de manière à empêcher toute intrusion non autorisée dans votre système de la part des tiers. Ce firewall devra être installé au niveau de votre routeur Wi-Fi, et s'ajoutera à celui déjà présent sur votre ordinateur.

La multiplication des réseaux Wi-Fi pose des problèmes de sécurité supplémentaires, dès lors que ces réseaux sont accessibles depuis l'extérieur. En effet, les ondes dépassent le périmètre d'utilisation normale du réseau. Il est donc nécessaire de protéger son réseau Wi-Fi, notamment en utilisant des dispositifs qui assurent le cryptage, l'authentification et l'identification des postes de travail accédant au réseau sans fil et des données y transitant. Des protocoles de sécurité tels que le WEP ou le WPA2 (Wi-Fi Protected Access 2) permettent de sécuriser le réseau et de rencontrer ces trois fonctions.

Ainsi, il est possible d'encrypter les informations qui transitent par le Wi-Fi, de les rendre invisibles aux tiers, ou encore de protéger votre accès par un mot de passe. En outre, il est également possible de ne relier votre routeur Wi-Fi qu'aux seuls ordinateurs identifiés. Ceci peut être réalisé en utilisant l'adresse MAC, qui est l'identifiant unique et mondial attribué à votre carte réseau. Seuls les ordinateurs ayant une adresse MAC répertoriée par le routeur Wi-Fi seront autorisés à accéder au routeur.

Aucune protection n'étant infaillible, il est recommandé de bien se renseigner auprès de son revendeur de routeur Wi-Fi ou de son fournisseur d'accès, ainsi que de bien lire les guides d'utilisation fournis avec le matériel afin d'optimiser au mieux la sécurité de son réseau sans fil.

Auteurs: FUNDP-CRID sous la coordination de Romain Robert

Fiche pratique

Comment installer un hotspot dans mon magasin au profit de mes clients ?

Si vous êtes propriétaire d'un bar ou d'un restaurant, ou encore d'un autre lieu fréquenté par le public, et que vous désirez permettre à vos clients de surfer sur Internet par le Wi-Fi, vous pouvez ouvrir votre accès Wi-Fi de manière à ce qu'ils puissent s'y connecter. Pour ce faire, vous pourrez par exemple restreindre l'accès par un mot de passe que vous donnerez à vos clients.

Relevons toutefois que les conditions générales de certains fournisseurs d'accès interdisent le partage de la connexion Internet avec des tiers. En outre, des problèmes de sécurité peuvent se poser dès lors qu'il est parfois difficile – voire impossible – d'identifier les personnes qui se sont connectées sur un point d'accès Wi-Fi ouvert.

Une autre solution consiste à faire de votre commerce un hotspot, et demander à un fournisseur d'accès (comme Telenet ou Belgacom) d'installer un point d'accès public qui permettra aux clients de se connecter à Internet au moyen de cartes prépayées que vous distribuez ou via un abonnement qu'ils auront directement souscrit auprès du fournisseurs d'accès.

Auteurs: FUNDP-CRID sous la coordination de Romain Robert

Le Wi-Fi - Internaute@Web: Questions

"Qu'est-ce que le Wi-Fi?"

"De quoi ai-je besoin pour surfer sans fil chez moi?"

"Comment accéder à Internet par le Wi-Fi si je ne dispose pas d'une connexion Internet à la maison?"

"Puis-je me connecter sur Internet par le réseau Wi-Fi de mon voisin sans son auto-risation?"

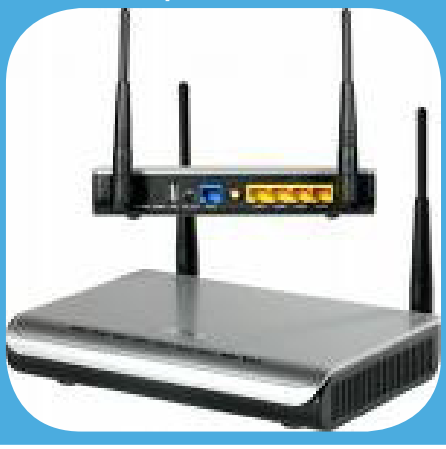
"Dois-je protéger mon accès Wi-Fi contre les intrusions non désirées?"

"Comment me protéger contre les accès non autorisés?"

"Les ondes Wi-Fi sont-elles dangereuses pour la santé?"

Fiche pratique

Qu'est-ce que le Wi-Fi ?



Le Wi-Fi (pour « Wireless Fidelity ») est une technique de communication en réseau local sans fil. Cette technique permet une connexion à haut débit entre des ordinateurs et des terminaux et est devenue un autre moyen d'accéder à Internet à haut débit.

Equipé d'une carte Wi-Fi (intégrée ou externe), votre ordinateur peut communiquer avec d'autres terminaux ou accéder à Internet avec une vitesse de connexion pouvant dépasser les 10 Mbps. Certains appareils portables, comme par exemple un téléphone portable ou un lecteur MP3 de dernière génération, sont également équipés d'une telle technologie.

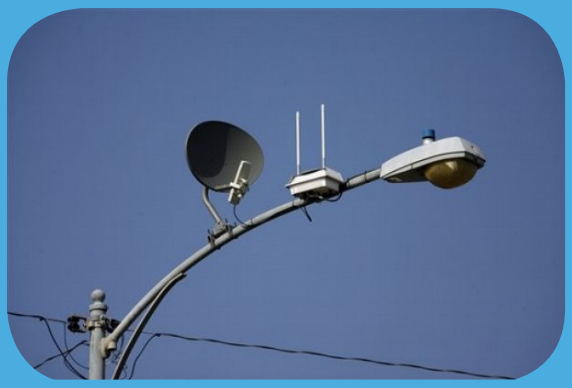
La portée des ondes Wi-Fi étant relativement réduite (plusieurs dizaines de mètres), cette norme est destinée à l'établissement d'un réseau sans fil local (contrairement au réseau GSM ou 3G par exemple).

La technologie Wi-Fi peut être utilisée à des fins purement domestiques (par exemple pour l'établissement d'un réseau local pour accéder sans fil à Internet). Il présente ainsi l'avantage de ne plus devoir tirer une multitude de câbles dans toute la maison pour surfer à plusieurs, ou pour relier votre ordinateur au modem ou à d'autres ordinateurs.

Par ailleurs, de plus en plus de fournisseurs d'accès à Internet et d'établissements divers (cafés, magasins, aéroports, bibliothèques…) installent des points d'accès Wi-Fi (ou « bornes Wi-Fi ») afin de permettre un accès à Internet haut débit dans les lieux publics. Ces lieux sont appelés hotspots et sont répertoriés sur Internet ou renseignés sur les lieux d'accès.

Auteurs: CRID, sous la coordination de Romain Robert

De quoi ai-je besoin pour surfer sans fil chez moi ?



Pour pouvoir surfer sans fil à la maison, vous devez bénéficier d'une connexion à Internet à haut débit, mais vous ne devez pas nécessairement effectuer de démarche particulière auprès de votre fournisseur d'accès à Internet. Il vous suffit de vous procurer le matériel adéquat dans n'importe quel magasin (« réel » ou virtuel) fournissant du matériel de télécommunication.

Pour bénéficier de la technologie Wi-Fi, il vous suffit de vous procurer un modem Wi-Fi ou un routeur Wi-Fi connecté à votre modem, et de vérifier que votre ordinateur est bien équipé d'une carte Wi-Fi. De plus en plus d'ordinateurs en vente sur le marché sont équipés d'une carte Wi-Fi interne. Si tel n'est pas le cas, il vous suffit de vous procurer une carte Wi-Fi externe compatible avec votre ordinateur, que vous relierez à celui-ci (par exemple au moyen d'un port USB).

Notez que si les produits en vente affichent parfois des débits théoriques de connexion impressionnants, le débit réel de votre connexion sera généralement inférieur (même s'il restera souvent confortable) et variera en fonction de certains éléments, comme la distance et les obstacles séparant l'ordinateur du point d'accès.

Il faudra enfin veiller à paramétrer correctement votre routeur afin qu'il puisse communiquer avec votre ordinateur (souvent, un CD-ROM d'installation « pas à pas » est fourni avec le matériel). Par la même occasion, veillez à sécuriser votre connexion Wi-Fi afin qu'elle ne soit accessible qu'aux seules personnes autorisées.

Le routeur ou le modem Wi-Fi fait office d'antenne qui émet dans les environs proches. Les ondes sont réceptionnées par la carte Wi-Fi de l'ordinateur. Le signal aura une portée pouvant aller de quelques mètres à plus de cent mètres, en fonction des obstacles et de l'environnement. Normalement, ce signal peut traverser la plupart des structures d'un immeuble (murs, cloisons, planchers, portes et fenêtres…), de sorte que vous pouvez le capter d'une pièce à l'autre, d'un étage à l'autre, ou de la maison au jardin. Cependant, certaines matières opposent une résistance plus forte (murs épais, béton armé, structures métalliques…) et peuvent perturber le signal. Veillez donc à choisir l'emplacement de votre point d'accès Wi-Fi en fonction de l'environnement, ou à placer des relais Wi-Fi en plusieurs points de votre maison si nécessaire.

Moyennant cette installation, il est possible de connecter plusieurs ordinateurs sur un même point d'accès, ce qui permet de partager la connexion Internet. Le Wi-Fi permet ainsi de créer un réseau interne, connectant entre eux des ordinateurs et autres terminaux sur une fréquence radio déterminée, au sein d'un même foyer ou d'une même entreprise.

Auteurs: CRID, sous la coordination de Romain Robert

Comment accéder à Internet par le Wi-Fi si je ne dispose pas d'une connexion Internet à la maison ?

Plusieurs fournisseurs d'accès à Internet, lieux publics et autres entités commerciales (les hôtels, les exploitants de cafés ou restaurants, les gares, les aéroports,...) ont installé des bornes Wi-Fi dans des zones très fréquentées, appelées hotspots, pour permettre à leurs clients d'accéder à Internet.

Pour pouvoir capter les signaux émis par les hotspots, il faut bien entendu que votre ordinateur (ou PDA) soit équipé d'une carte Wi-Fi, que vous pouvez vous procurer dans n'importe quel magasin (« réel » ou virtuel) fournissant du matériel de télécommunication. En dehors de cela, aucun logiciel spécifique n'est nécessaire.

Cet accès Wi-Fi est proposé soit gratuitement, soit contre rémunération.

L'accès payant est possible par le biais de cartes prépayées ou d'abonnements qui peuvent notamment être achetés auprès du fournisseur d'accès à Internet qui relie la borne Wi-Fi à Internet (comme Telenet ou Belgacom, qui disposent tous deux d'un certain nombre de hotspots dans plusieurs lieux publics). L'utilisateur recevra alors un identifiant et un mot de passe pour se connecter aux bornes Wi-Fi gérées par le fournisseur. Il existe plusieurs sites web qui répertorient la liste des hotspots dans le monde et permettent de trouver la borne la plus proche de sa localisation ainsi que les modalités d'accès à la borne (par exemple : http://www.jiwire.com, ou http://www.trustive.com/hotspots/).

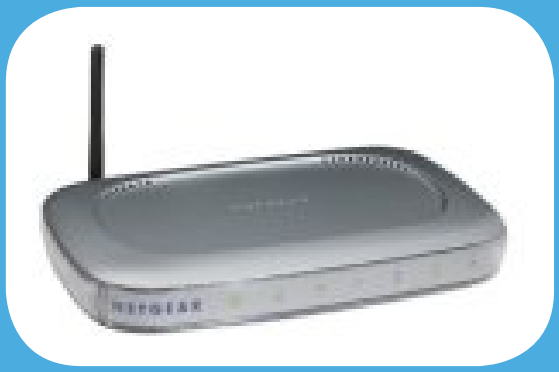
Certains hôtels ou café laissent, quant à eux, un accès libre à leur réseau Wi-Fi pour permettre à leurs clients de surfer sur Internet. Ces accès impliquent parfois de connaître le mot de passe pour se connecter au réseau.

Signalons également l'existence de communautés Wi-Fi où les membres partagent leur accès à Internet via leur connexion Wi-Fi. Un exemple de communauté Wi-Fi est la communauté FON (www.fon.com): les membres partagent gratuitement leur connexion Internet entre eux. Les non membres, quant à eux, peuvent avoir accès aux bornes des membres moyennant paiement.

Auteurs: CRID, sous la coordination de Romain Robert

Fiche pratique

Puis-je me connecter sur Internet par le réseau Wi-Fi de mon voisin sans son autorisation ?



La loi punit les accès réalisés dans des systèmes informatiques tout en sachant que l'on y est pas autorisé. Dès lors, en cas d'accès à un réseau sans autorisation explicite, se posera la question de savoir si le tiers « savait qu'il n'y était pas autorisé », puisque tel est l'élément qui est repris dans le texte de la loi et qui déterminera si l'intrusion est illégale ou non.

Notez que le fait pour un tiers de ne pas sécuriser son système ne veut pas dire que cette personne vous autorise à accéder à son réseau librement, ni à profiter de sa connexion à Internet gratuitement.

Pour votre défense, vous pourriez prétendre que vous ignoriez ne pas être autorisé à utiliser le réseau Wi-Fi d'un tiers. On pourrait en effet avancer que l'usage libre d'un point d'accès Wi-Fi est relativement courant en milieu urbain (hotspots gratuits) ou encore que sans protection de son réseau, le titulaire de l'accès devrait être présumé accepter que des tiers s'y connectent.

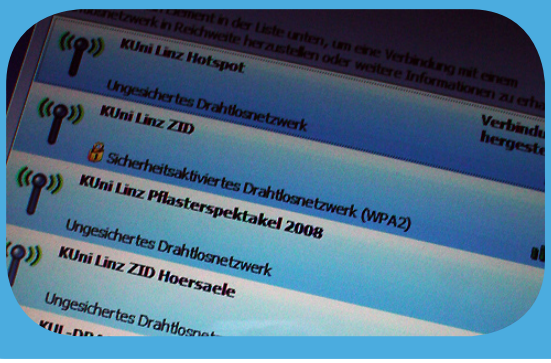
Néanmoins, rien ne permet de conclure que le titulaire d'un accès à Internet consentirait par défaut au partage de cet accès via son routeur Wi-Fi, dans le cas où il n'aurait pas expressément émis d'interdiction à cet égard. En outre, il n'est pas requis qu'il existe un dispositif de protection et que celui-ci soit contourné pour qu'il y ait infraction.

Vous pourriez aussi prétendre que vous ignoriez être branché sur le réseau Wi-Fi d'un tiers. Ce dernier argument sera néanmoins difficilement convaincant dès lors que devriez légitimement vous rendre compte que vous accédez à Internet sans avoir souscrit d'abonnement.

De plus, rappelons que les forfaits Internet sont souvent limités à un certain volume mensuel. Utiliser la connexion d'un tiers peut donc rapidement épuiser son forfait et lui coûter cher, puisque chaque Gigabyte au-delà du volume mensuel lui sera généralement facturée. Le dommage qui résulte de l'utilisation frauduleuse de la connexion d'un tiers pourrait donc faire l'objet d'une demande de dédommagement de la part du titulaire de l'accès à Internet illicitement utilisé.

Auteurs: CRID, sous la coordination de Romain Robert

Dois-je protéger mon accès Wi-Fi contre les intrusions non désirées ?



La question de la sécurité des réseaux Wi-Fi est fréquemment soulevée. En effet, l'accès sans fil permet aux tiers d'accéder à un système plus facilement puisque les ondes émises par le routeur ne se limitent pas à un périmètre bien défini. Par conséquent, il leur sera plus facile de s'y introduire que sur un réseau filaire, où la seule possibilité pour se connecter est de se brancher « physiquement » sur ce réseau.

Il se peut que votre fournisseur d'accès vous facture des montants supplémentaires pour avoir dépassé le volume mensuel maximum inclus dans votre forfait. Laisser un tiers surfer sur votre compte Internet risque donc d'augmenter votre facture mensuelle.

Enfin, si un acte illégal est commis par le biais de votre connexion Wi-Fi par un tiers, il sera peut-être difficile, voire impossible pour les autorités judiciaires d'identifier l'auteur de l'infraction, sans compter que le premier suspect sera souvent le titulaire de la connexion Internet identifiée, à savoir... vous.

Il est donc primordial de protéger votre ordinateur et votre système Wi-Fi contre les intrusions non désirées. Les modes d'emploi des routeurs Wi-Fi et certains fournisseurs d'accès donnent de précieuses instructions pour sécuriser son réseau. L'encryptage des données et l'identification des ordinateurs qui peuvent se connecter au réseau Wi-Fi figurent parmi ces méthodes de protection.

Auteurs: CRID, sous la coordination de Romain Robert

Comment me protéger contre les accès non autorisés ?

Certains surfeurs sur Internet sont passés maîtres dans l'art de pénétrer les systèmes informatiques connectés au réseau, parfois par jeu, pour relever un défi ou, tout simplement, pour nuire ou semer la pagaille. Il serait naïf de vous croire à l'abri de pareils agissements, sous prétexte que vous n'avez rien à vous reprocher ou que votre système ne contient rien de bien extraordinaire.

De manière générale, pour vous protéger, le mieux est d'installer un firewall (pare-feu), c'est-à-dire un dispositif, logiciel ou matériel, destiné précisément à dresser un mur de sécurité entre votre système et le reste du réseau, de manière à empêcher toute intrusion non autorisée dans votre système de la part des tiers. Ce firewall devra être installé au niveau de votre routeur Wi-Fi, et s'ajoutera à celui déjà présent sur votre ordinateur.

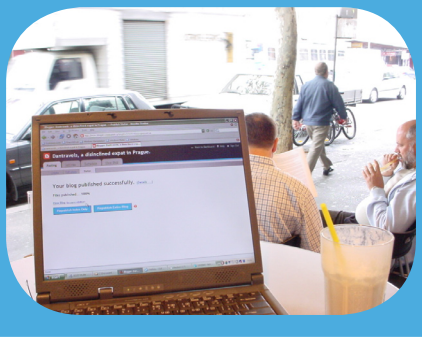
La multiplication des réseaux Wi-Fi pose des problèmes de sécurité supplémentaires, dès lors que ces réseaux sont accessibles depuis l'extérieur. En effet, les ondes dépassent le périmètre d'utilisation normale du réseau. Il est donc nécessaire de protéger son réseau Wi-Fi, notamment en utilisant des dispositifs qui assurent le cryptage, l'authentification et l'identification des postes de travail accédant au réseau sans fil et des données y transitant. Des protocoles de sécurité tels que le WEP ou le WPA2 (Wi-Fi Protected Access 2) permettent de sécuriser le réseau et de rencontrer ces trois fonctions.

Ainsi, il est possible d'encrypter les informations qui transitent par le Wi-Fi, de les rendre invisibles aux tiers, ou encore de protéger votre accès par un mot de passe. En outre, il est également possible de ne relier votre routeur Wi-Fi qu'aux seuls ordinateurs identifiés. Ceci peut être réalisé en utilisant l'adresse MAC, qui est l'identifiant unique et mondial attribué à votre carte réseau. Seuls les ordinateurs ayant une adresse MAC répertoriée par le routeur Wi-Fi seront autorisés à accéder au routeur.

Aucune protection n'étant infaillible, il est recommandé de bien se renseigner auprès de son revendeur de routeur Wi-Fi ou de son fournisseur d'accès, ainsi que de bien lire les guides d'utilisation fournis avec le matériel afin d'optimiser au mieux la sécurité de son réseau sans fil.

Auteurs: CRID, sous la coordination de Romain Robert

Les ondes Wi-Fi sont-elles dangereuses pour la santé ?



Comme toute propagation d'ondes électromagnétiques, la question de l'impact des ondes Wi-Fi sur la santé est fréquemment soulevée.

La question de la dangerosité des réseaux sans fil (GSM, WIMAX, UMTS, Wi-FI,…) ne semble pas faire l'unanimité. Toutefois, elle est de plus en plus souvent prise en compte par les pouvoirs publics et fait l'objet de nombreuses réflexions à ce jour.

Ainsi, plusieurs études sur la dangerosité des ondes ont été menées. Mentionnons celle de l'Organisation Mondiale de la Santé, qui a publié un « Aide-mémoire sur les Champs électromagnétiques et la santé publique » (http://www.who.int/mediacentre/factsheets/fs304/fr/index.html), en abordant spécifiquement la question de l'hypersensibilité électromagnétique (EHS).

Le régulateur télécom français a commandé une étude « RLAN et Champs électromagnétiques » (http://www.arcep.fr/uploads/tx_gspublication/synth-etudesupelec-wifi-dec06.pdf) dans lequel figurent également plusieurs recommandations pour s'exposer au minimum aux ondes Wi-Fi (par exemple: débrancher le routeur Wi-Fi la nuit, ne pas s'interposer entre la borne et l'ordinateur,..).

Citons également certains site dédiés à cette question, comme celui du Centre de Recherche et d'Information Indépendantes sur les Rayonnements ElectroMagnétiques (http://riimem.blogspirit.com/), ou encore de la Fondation Santé et Radiofréquence (http://www.sante-radiofrequences.org/).

Auteurs: CRID, sous la coordination de Romain Robert